

Families of Optimal Binary Non-MDS Erasure Codes

Danilo Gligoroski and Katina Kralevska

Department of Telematics, Faculty of Information Technology, Mathematics and Electrical Engineering,
Norwegian University of Science and Technology, Trondheim, Norway,
Email: {danilog, katinak}@item.ntnu.no

Abstract—We introduce a definition for *Families of Optimal Binary Non-MDS Erasure Codes* for $[n, k]$ codes over $GF(2)$, and propose an algorithm for finding those families by using hill climbing techniques over Balanced XOR codes. Due to the hill climbing search, those families of codes have always better decoding probability than the codes generated in a typical Random Linear Network Coding scenario, i.e., random linear codes. We also show a surprising result that for small values of k , the decoding probability of our codes in $GF(2)$ is very close to the decoding probability of the codes obtained by Random Linear Network Coding but in the higher finite field $GF(4)$.

I. INTRODUCTION

In the fast approaching Zettabyte Era [3] the erasure codes will become the most important codes among all coding techniques. That is mostly due to two factors: 1. The global communications will be almost exclusively based on the packet switching paradigm, where the recovery from packet losses is addressed efficiently by erasure codes; 2. Storage systems will have capacities of hundreds of exabytes, and will have to tolerate and recover efficiently from multiple disk failures.

According to the rate of redundancy that is used, the erasure codes are divided in two classes: 1. Optimal or very close to optimal ones, known as Maximum Distance Separable (MDS) Codes [19], almost-MDS (AMDS) [5] and near-MDS codes (NMDS) [6], and 2: Suboptimal or non-MDS codes [7], [8], [11], [14], [17].

Reed-Solomon codes [22] are a well known class of MDS codes that provide a general technique for construction of MDS codes. However, these codes are defined in higher finite fields and they can be very computationally demanding. That is the main reason for series of research efforts to find codes that work just in the simplest finite field $GF(2)$ where the operations are bitwise exclusive-or (XOR) operations [2], [4], [12], [13].

Beside the use in massive storage systems, the erasure codes have been recently used in one research area that is addressing the demanding needs for increasing the speed and reliability of packet based communications. That evolving area is Network Coding [1]. Network Coding allows nodes in the network to perform a set of functions over the generated or received data packets before forwarding them. Random Linear Network Coding (RLNC) [10] is a network coding technique that produces random linear combinations of the packets over

a Galois Field of size q , $GF(q)$. The field size has an impact on the decoding probability, i.e., the probability of receiving linearly independent packets increases with q .

When one or more sources want to transmit k packets to one or more destination nodes, the channel conditions must be considered. Even in a presence of packet losses (erasures) the destination node has to be able to decode k original packets by receiving $k+r$ packets. The authors in [18] derive the average number of received coded packets n for successful decoding of k original packets at the destination nodes. They study the effect of q on the performance of RLNC. The exact probability that k out of $k+r$ received packets are linearly independent is derived in [24]. Both papers show that q equal to 4 or 8 is enough to get very close to the optimal performance even when k is not very large.

However, as in the case of codes for massive storage systems, working in higher fields or with large number of data packets has an impact on the computational complexity leading to higher energy consumption [9] and no real benefits. A recent result in [21] shows that the speed of computation on modern CPUs with wide SIMD instructions is similar for operations in $GF(2)$ and in $GF(16)$. On the other hand, implementing RLNC in higher fields on devices that have power and memory constraints is a challenging problem. Some recent studies show that RLNC in constrained devices in $GF(2)$ is up to two orders of magnitude less energy demanding and up to one order of magnitude faster than RLNC in higher fields [25], [20].

In this work we introduce a definition of *Families of Optimal Binary Non-MDS Erasure Codes* for $[n, k]$ codes over $GF(2)$. Then we propose one heuristic algorithm for finding those families by using hill climbing techniques over Balanced XOR codes introduced in [15]. Due to the hill climbing search, those families of codes have always better decoding probability than the codes generated in a typical Random Linear Network Coding scenario, i.e., random linear codes as described in [24]. We also show a surprising result that for small values of k , the decoding probability of our codes in $GF(2)$ is very close to the decoding probability of the codes obtained by RLNC but in the higher finite field $GF(4)$.

The paper is organized as follows. In Section II, we introduce the basic terminology and the definition of Families of Optimal Binary Non-MDS Erasure Codes. In Section III, we

describe one heuristic algorithm for finding those Families of Optimal Binary non-MDS Erasure Codes. We also discuss and compare the properties of our erasure codes to codes generated in a typical Random Linear Network Coding scenario, i.e., random linear codes. Conclusions and future work are summarized in Section IV.

II. MATHEMATICAL PRELIMINARIES

In this section we briefly introduce the basic terminology, some useful properties and facts about linear codes, as well as some basic terminology and coding methods for Balanced XOR codes [15].

Let us denote by $\mathbf{F}_q = GF(q)$ the Galois field with q elements, and by \mathbf{F}_q^n the n -dimensional vector space over \mathbf{F}_q . Let us also denote by $[n, k]_q$ the q -ary linear code of length n and rank k which is actually a linear subspace C with dimension k of the vector space \mathbf{F}_q^n . An $[n, k, d]_q$ code is an $[n, k]_q$ code with minimum weight at least d among all nonzero codewords. An $[n, k, d]_q$ code is called maximum distance separable (MDS) if $d = n - k + 1$. The Singleton defect of an $[n, k, d]_q$ code C defined as $s(C) = n - k + 1 - d$ measures how far away is C from being MDS.

Below we give some basic properties for MDS matrices that we use in this paper:

Proposition 1 ([19], Ch. 11, Corollary 3): Let C be an $[n, k, d]_q$ code over $GF(q)$. The following statements are equivalent:

- 1) C is MDS;
- 2) every k columns of a generator matrix G are linearly independent;
- 3) every $n - k$ columns of a parity check matrix H are linearly independent.

Definition 1: Let C be an $[n, k]$ code over $GF(q)$ with a generator matrix G . Let us denote by $\mathcal{G}_I, I = k, \dots, n$ the sets of submatrices obtained from G when choosing I columns from G , and by $\mathcal{D}_I \subset \mathcal{G}_I, I = k, \dots, n$ the subsets of \mathcal{G}_I with a rank k . We call the following vector $V_D = (\varrho_0, \varrho_1, \dots, \varrho_{n-k}), \varrho_i = |\mathcal{D}_{i+k}|/|\mathcal{G}_{i+k}|$, the *Vector of Exact Decoding Probability*, for the code C .

With other words, the value ϱ_i represents the probability that we can decode all k original values x_1, \dots, x_k , if we are given $k + i$ values y_1, \dots, y_{k+i} that corresponds to encoding with $k + i$ columns of the generator matrix G .

For random generator matrices G , the values of V_D are calculated in [24] and we formulate them in the following Proposition:

Proposition 2: For a linear $[n, k]$ code over $GF(q)$ with a random generator matrix G the elements of the vector $V_D = (\varrho_0, \varrho_1, \dots, \varrho_{n-k})$ have the following values:

$$\varrho_i = P(k + i), \quad (1)$$

where the values $P(I)$ are computed as follows:

$$P(I) = \begin{cases} 0 & \text{if } I < k, \\ \prod_{j=0}^{k-1} \left(1 - \frac{1}{q^{I-j}}\right) & \text{if } I \geq k. \end{cases} \quad (2)$$

Proof: The equation (2) is actually the equation (7) in [24] with adopted notation to be consistent with the standard notation for linear $[n, k]$ codes over $GF(q)$. The equation (1) then follows directly. ■

The connection between the Vector of Exact Decoding Probability and the MDS codes can be established by using the Proposition 2 as follows:

Theorem 1: A linear $[n, k]$ code C over $GF(q)$ with a generator matrix G is a MDS code iff the Vector of Exact Decoding Probability is the following vector $V_D = (\varrho_0, \varrho_1, \dots, \varrho_{n-k}) = (1, 1, \dots, 1)$.

Proof: The theorem can be proved with a direct application of the Proposition 2 and the Definition 1. ■

In this work we are interested exclusively to work with XOR coding, i.e., to work with linear binary codes. Thus, our interest is to define a class of binary codes that in some properties are as close as possible to MDS codes. Unfortunately, it is a well known old fact in coding theory (see for example [19]) that for the case of linear binary codes, all MDS codes are trivial, i.e., $k = 1$ or $n = k + 1$ or $n = k$.

So, dealing with the fact that non-trivial binary codes are not MDS, we adopt a strategy to search for codes that will be optimal from certain perspective according to the Vector of Exact Decoding Probability V_D . When a channel has an erasure probability p the strategy will be to find binary codes that maximize the probability to recover the original data. Therefore, we prove the following Theorem:

Theorem 2: Let C be a binary linear $[n, k]$ code with a Vector of Exact Decoding Probability $V_D = (\varrho_0, \varrho_1, \dots, \varrho_{n-k})$ and let k packets are encoded by C . The probability p_s of successful decoding of k packets from n encoded and transmitted packets via a channel with an erasure probability p is:

$$p_s = 1 - \left(\sum_{i=0}^{n-k} \binom{n}{i} p^i (1-p)^{n-i} (1-\varrho_{n-k-i}) + \sum_{i=n-k+1}^n \binom{n}{i} p^i (1-p)^{n-i} \right) \quad (3)$$

Proof: Let us denote by E_1 the event that i packets, where $0 \leq i \leq n - k$, are lost during the transmission, and by E_2 the event that more than $n - k$ packets from the set of all n packets are lost during the transmission.

The probability of the event E_1 is calculated by the expression:

$$P(E_1) = \sum_{i=0}^{n-k} \binom{n}{i} p^i (1-p)^{n-i}, \quad (4)$$

and the probability of the event E_2 is:

$$P(E_2) = \sum_{i=n-k+1}^n \binom{n}{i} p^i (1-p)^{n-i}. \quad (5)$$

From expression (4) we compute the probability p_{u_1} of failure to decode k original packets, by multiplying every value in the sum by the opposite probability of successful decoding when $n - k - i$ columns of the generator matrix G are received, i.e., when i packets are lost. So the decoding failure probability

if i packets are lost ($0 \leq i \leq n - k$) is computed by the following expression:

$$p_{u_1} = \sum_{i=0}^{n-k} \binom{n}{i} p^i (1-p)^{n-i} (1 - \varrho_{n-k-i}). \quad (6)$$

If more than $n - k$ packets are lost then the probability to fail the decoding is 100% thus the probability p_{u_2} of failure to decode k original packets is equal to $P(E_2)$, i.e., $p_{u_2} = P(E_2)$.

In total, the probability of unsuccessful decoding p_u is:

$$\begin{aligned} p_u &= p_{u_1} + p_{u_2} = \\ &= \sum_{i=0}^{n-k} \binom{n}{i} p^i (1-p)^{n-i} (1 - \varrho_{n-k-i}) + \\ &\quad + \sum_{i=n-k+1}^n \binom{n}{i} p^i (1-p)^{n-i} \end{aligned} \quad (7)$$

Finally the probability p_s of successful decoding of k packets is the opposite probability of p_u i.e.,

$$p_s = 1 - p_u.$$

Having defined the probability p_s of successful decoding of k packets that are encoded with an $[n, k]$ binary code, we define a *Family of Optimal Binary Non-MDS Erasure Codes* as follows:

Definition 2: Let \mathcal{C} be a family of binary linear $[n, k]$ codes that have a probability p_s of successful decoding k packets from n encoded and transmitted packets via a channel with an erasure probability p . We say that \mathcal{C} is a *Family of Optimal Binary Non-MDS Erasure Codes* if for every binary linear $[n, k]$ code C' with a probability p'_s of successful decoding of k packets in a channel with an erasure probability p , there exist a code $C \in \mathcal{C}$ with a probability p_s of successful decoding, such that $p'_s \leq p_s$, for every erasure probability p .

Problem 1: For given values of n and k find a Family \mathcal{C} of Optimal Binary Non-MDS Erasure Codes.

III. A HILL CLIMBING HEURISTICS FOR FINDING FAMILIES OF OPTIMAL BINARY NON-MDS ERASURE CODES

Finding exact analytical solution (or finding deterministic and efficient algorithm that will find the solution) for the Problem 1 is hard and in this moment we do not know such a solution. However, there are many heuristic optimization methodologies that can be used for a search of approximate solutions. We choose to use the simplest one: The Stochastic Hill-Climbing Methodology [23]. The hill climbing heuristics has been already used in optimizing problems for RLNC such as in [16]. In general, the stochastic heuristics is defined as in Algorithm 1.

In order to improve the codes found by Algorithm 1 we decided to work with balanced structures as they were introduced in [15].

TABLE I
A GENERAL STOCHASTIC HILL-CLIMBING ALGORITHM FOR FINDING A FAMILY OF OPTIMAL BINARY NON-MDS ERASURE CODES FOR GIVEN VALUES OF n AND k

Algorithm 1
Input. n and k
Output. A candidate Family \mathcal{C} of Optimal Binary Non-MDS Erasure Codes
<ol style="list-style-type: none"> 1. Find a random $[n, k]$ linear binary code and compute its Vector of Exact Decoding Probability $V_D = (\varrho_0, \varrho_1, \dots, \varrho_{n-k})$ and its probability p_s of successful decoding of k packets from the equation (3). 2. Repeatedly improve the solution until no more improvements are necessary/possible.

Definition 3: A XOR-ed coding is a coding that is realized exclusively by bitwise XOR operations between packets with equal length. Hence, it is a parallel bitwise linear transformation of k source bits $x = (x_1, \dots, x_k)$ by a $k \times k$ nonsingular binary matrix \mathbf{K} , i.e., $y = x \cdot \mathbf{K}$.

In other words XOR-ed coding assumes work within the smallest finite field $GF(2)$, i.e., with $k \times k$ nonsingular binary matrices \mathbf{K} . While the binary matrices \mathbf{K} in general can be of any form, the specifics about matrices introduced in [15] are that they are highly structured, balanced and their construction is based on Latin rectangles of dimensions $k_1 \times k$.

Definition 4: A Latin square of order k with entries from an k -set X is an $k \times k$ array L in which every cell contains an element of X such that every row of L is a permutation of X and every column of L is a permutation of X .

Definition 5: A $k_1 \times k$ Latin rectangle is a $k_1 \times k$ array (where $k_1 \leq k$) in which each cell contains a single symbol from an k -set X , such that each symbol occurs exactly once in each row and at most once in each column.

Definition 6: Let (X, A) be a design where $X = \{x_1, \dots, x_v\}$ and $A = \{A_1, \dots, A_b\}$. The incidence matrix of (X, A) is the $v \times b$ 0-1 matrix $M = (m_{i,j})$ defined by the rule $m_{i,j} = \begin{cases} 1, & \text{if } x_i \in A_j, \\ 0, & \text{if } x_i \notin A_j. \end{cases}$

Proposition 3 ([15]): The incidence matrix $M = (m_{i,j})$ of any Latin rectangle with dimensions $k_1 \times k$ is a balanced matrix with k_1 ones in each row and each column.

Proposition 4 ([15]): The necessary condition an incidence matrix $M = (m_{i,j})$ of a $k_1 \times k$ Latin rectangle to be nonsingular in $GF(2)$ is k_1 to be odd, i.e., $k_1 = 2l + 1$.

Example 1: Let us take the following Latin square and split it into two Latin rectangles:

$$L = \begin{bmatrix} 1 & 4 & 3 & 5 & 2 \\ 3 & 1 & 5 & 2 & 4 \\ 4 & 2 & 1 & 3 & 5 \\ 5 & 3 & 2 & 4 & 1 \\ 2 & 5 & 4 & 1 & 3 \end{bmatrix}.$$

The incidence matrix M of the 3×5 upper Latin rectangle is:

$$M = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Note how balanced are the rows and columns: in every row and every column, the number of 1s is 3.

The following proposition follows directly from the Proposition 4:

Proposition 5: The $k+1$ -th column of the generator matrix G of a trivial $[k+1, k]_2$ MDS code that has in the first k columns a matrix for a balanced XOR-ed coding consists of all 1s.

We now describe the modified Stochastic Hill-Climbing that is using Balanced XOR codes where one column of the generator matrix is defined as in Proposition 5:

TABLE II
A STOCHASTIC HILL-CLIMBING ALGORITHM FOR FINDING A FAMILY OF OPTIMAL BINARY NON-MDS ERASURE CODES BASED ON BALANCED XOR CODES

Algorithm 2
Input. n and k
Output. A candidate Family \mathcal{C} of Optimal Binary Non-MDS Erasure Codes
<ol style="list-style-type: none"> 1. Find a random Balanced XOR code and put it as the first part of the generator matrix G of an $[n, k]$ code. Set the $k+1$-th column to consists of all 1s, and set the remaining columns with random values. Compute the Vector of Exact Decoding Probability $V_D = (\varrho_0, \varrho_1, \dots, \varrho_{n-k})$ and its probability p_s of successful decoding of k packets from the equation (3). 2. Repeatedly improve the solution until no more improvements are necessary/possible.

We would like to note that Algorithm 1 can find codes with similar decoding probabilities as Algorithm 2, but after performing more stochastic search attempts. Moreover, the codes that Algorithm 2 finds have advantages that they are structured, balanced and they are sparse, where the sparsity can go down to just 3 nonzero positions.

We now give two numerical results that compare the performance of our codes to a typical linear random code in $GF(2)$ that can be generated in RLNC. The same parameters are taken as in [24], i.e., $r = 0, \dots, 8$ is the number of excess packets for $k = 5$ and $k = 100$. The results show that the decoding probability with our scheme is closer to the decoding probability under RLNC in $GF(4)$ when k is small. We would like to emphasize that with Algorithm 2 we could easily find codes with k in range $[5, \dots, 1000]$.

In Figure 1 the code that was found after 10,000 stochastic attempts by the Balanced XOR-ed approach of Algorithm 2 is based on the Latin Square from Example 1. Its generator

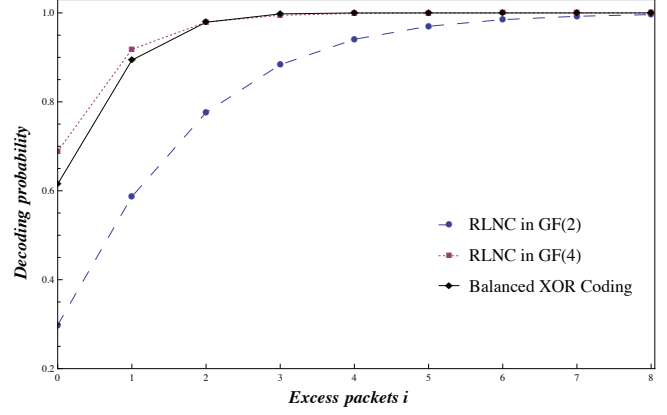


Fig. 1. Vector of Exact Decoding Probability V_D for $k=5$

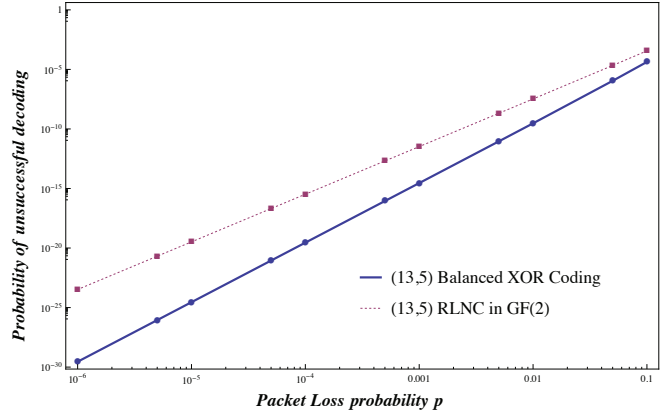


Fig. 2. Comparison between probabilities of unsuccessful decoding of a typical RLNC code and a code obtained with our stochastic strategy in $GF(2)$ for $k = 5$

matrix is the following:

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

The Vector of Exact Decoding Probability for this code is: $V_D = (0.615, 0.895, 0.979, 0.998, 1., 1., 1., 1.)$ and is presented in Figure 1 with a solid line.

A typical random linear code in $GF(2)$ generated in RLNC is presented in Figure 1 with a dashed line. For comparison purposes, we put the values for decoding probabilities of a typical random linear code in $GF(4)$ in the same Figure 1. As it can be seen, our codes in $GF(2)$ have decoding probabilities as a random linear code in $GF(4)$.

The real advantage of our codes is seen in Figure 2 in channels where packet losses occur with certain probabilities. Similarly as in [24] we give the results for $[n, k] = [108, 100]$ in Figure 3 and in Figure 4.

IV. CONCLUSIONS

We introduced a definition of *Families of Optimal Binary Non-MDS Erasure Codes* for $[n, k]$ codes over $GF(2)$ and

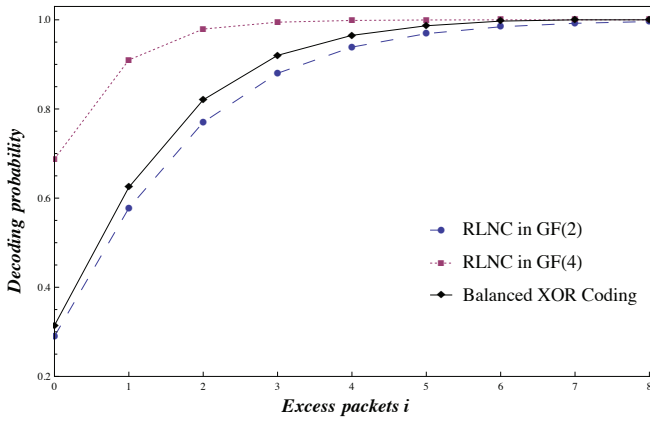


Fig. 3. Vector of Exact Decoding Probability V_D for $k=100$

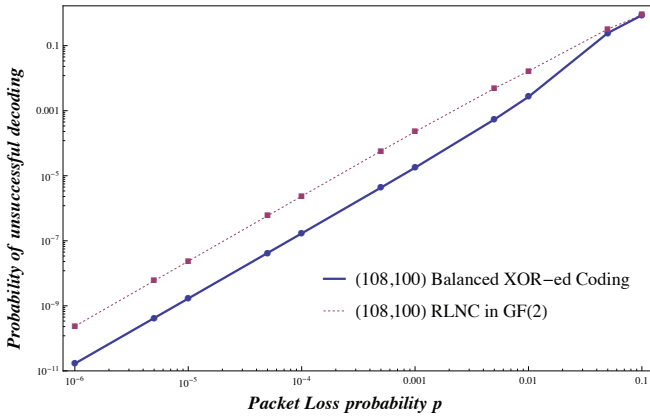


Fig. 4. Comparison between probabilities of unsuccessful decoding of a typical RLNC code and a code obtained with our stochastic strategy in $GF(2)$ for $k = 100$

proposed one heuristic algorithm for finding those families using hill climbing techniques over Balanced XOR codes. We showed that the families of codes that we found have always better decoding probability than the decoding probability of random linear codes generated in RLNC. We also showed that for small values of k the decoding probability of our codes in $GF(2)$ is very close to the decoding probability of the random linear codes in $GF(4)$.

As a next research direction, we point out that it will be very useful to further investigate the theoretical lower and upper bounds of decoding probabilities of the defined Families of Optimal Binary Non-MDS Erasure Codes and to find better heuristic or deterministic algorithms for efficient finding of those families. It would be a natural research directions to see how this methodology performs in higher fields.

ACKNOWLEDGEMENTS

We would like to thank Harald Øverby and Rune E. Jensen for their discussions that improved the quality of this paper. We would also like to thank the anonymous reviewers for their useful comments and suggestions.

REFERENCES

- [1] R. Ahlswede, N. Cai, S. Y. R. Li, and R. W. Yeung. Network information flow. *IEEE Transactions on Information Theory*, 46(4):1204–1216, 2000.
- [2] Mario Blaum, Jim Brady, Jehoshua Bruck, and Jai Menon. Evenodd: An efficient scheme for tolerating double disk failures in raid architectures. *IEEE Trans. Computers*, 44(2):192–202, 1995.
- [3] Cisco. Cisco visual networking index: Forecast and methodology, 20122017. *White Paper*, May 2013.
- [4] Peter F. Corbett, Robert English, Atul Goel, Tomislav Grcanac, Steven Kleiman, James Leong, and Sunitha Sankar. Row-diagonal parity for double disk failure correction. In *FAST*, pages 1–14. USENIX, 2004.
- [5] Mario A. de Boer. Almost mds codes. *Des. Codes Cryptography*, 9(2):143–155, 1996.
- [6] S.M. Dodunekov and I.N. Landjev. On near-mds codes. *Journal of Geometry*, 54:30–43, 1995.
- [7] Kevin M. Greenan, Xiaozhou Li, and Jay J. Wylie. Flat xor-based erasure codes in storage systems: Constructions, efficient recovery, and tradeoffs. In *MSST*, pages 1–14. IEEE Computer Society, 2010.
- [8] James Lee Hafner. Weaver codes: Highly fault tolerant erasure codes for storage systems. In *FAST*. USENIX, 2005.
- [9] Janus Heide, Morten V. Pedersen, Frank H. P. Fitzek, and Muriel Médard. On code parameters and coding vector representation for practical RLNC. In *ICC*, pages 1–5. IEEE, 2011.
- [10] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong. A random linear network coding approach to multicast. *IEEE Transactions on Information Theory*, 52(10):4413–4430, 2006.
- [11] Cheng Huang, Minghua Chen, and Jin Li. Pyramid codes: Flexible schemes to trade space for access efficiency in reliable data storage systems. *TOS*, 9(1):3, 2013.
- [12] Cheng Huang and Lihao Xu. Star : An efficient coding scheme for correcting triple storage node failures. *IEEE Trans. Computers*, 57(7):889–901, 2008.
- [13] O. Khan, R. Burns, J. S. Plank, W. Pierce, and C. Huang. Rethinking erasure codes for cloud file systems: Minimizing I/O for recovery and degraded reads. In *FAST-2012: 10th Usenix Conference on File and Storage Technologies*, San Jose, February 2012.
- [14] A. Kiani and S. Akhlaghi. A non-mds erasure code scheme for storage applications. *Journal of Communication Engineering*, 2.
- [15] K. Kralevska, D. Gligoroski, and H. Øverby. Balanced XOR-ed coding. In *Advances in Communication Networking - 19th EUNICE/IFIP*, volume 8115 of *LNCS*, pages 161–172. Springer, 2013.
- [16] E. Kurdoglu, N. Thomos, and P. Frossard. Scalable video dissemination with prioritized network coding. In *Multimedia and Expo (ICME), 2011 IEEE International Conference on*, pages 1–6, 2011.
- [17] Michael Luby, Michael Mitzenmacher, Mohammad Amin Shokrollahi, Daniel A. Spielman, and Volker Stemann. Practical loss-resilient codes. In *STOC*, pages 150–159. ACM, 1997.
- [18] Daniel Enrique Lucani, Muriel Médard, and Milica Stojanovic. Random linear network coding for time-division duplexing: Field size considerations. In *GLOBECOM*, pages 1–6. IEEE, 2009.
- [19] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-holland Publishing Company, 2nd edition, 1978.
- [20] M. V. Pedersen, J. Heide, F.H.P. Fitzek, and T. Larsen. Network coding for mobile devices - systematic binary random rateless codes. In *Workshop on Cooperative Mobile Networks 2009 - ICC09*. IEEE, June 2009.
- [21] J. S. Plank, K. M. Greenan, and E. L. Miller. Screaming fast Galois Field arithmetic using Intel SIMD instructions. In *FAST-2013: 11th Usenix Conference on File and Storage Technologies*, San Jose, February 2013.
- [22] Irving Reed and Golomb Solomon. Polynomial codes over certain finite fields. *Journal of the Society of Industrial and Applied Mathematics*, 8(2):300–304, 06/1960 1960.
- [23] S. Russel and P. Norvig. *Artificial Intelligence: A Modern Approach*. Pearson Education Inc., 2003.
- [24] Oscar Trullols-Cruces, Jose Maria Barcelo-Ordinas, and Marco Fiore. Exact decoding probability under random linear network coding. 2011.
- [25] P. Vingelmann, M. V. Pedersen, F. H. P. Fitzek, and J. Heide. Multimedia distribution using network coding on the iphone platform. *Proceedings of the 2010 ACM multimedia workshop on Mobile cloud media computing*, 2010.